Get a Grip --- On Computer Assets!

August 2006

There are things that people manage not to loose. Super Bowl passes, plane tickets to Tahiti, pictures of loved ones and family heirlooms are good examples of things rarely misplaced. Yet, official government computer assets do not seem to fall into this category.

The headlines and evening news reports are filled with stories of lost computers containing valuable and sensitive data that could compromise the identity and safety of thousands of people. This is unfortunately true of Army computer equipment as well. There appears to be two main causes for the loss of valuable computer hardware by Army personnel and contractors: carelessness and misplaced entrepreneurial spirit.

Carelessness is a human characteristic. Few of us have not left our wallet, car keys or briefcase somewhere when we were in a hurry or distracted. Usually we can just go back and reclaim it. Sometimes it is lost for good and that leads to a difficult, time-consuming process to recreate those lost items, a lesson that's not likely to be forgotten very soon. However, the more valuable an object is the more closely one usually guards it. It may come as a surprise that Army computers and memory devices are often lost or stolen due to irresponsibility. Some are even sold illegally by the very people to whom these assets were entrusted. What makes it more surprising is that many of these devices contain information that could put soldiers in danger.

Computers and related equipment are obviously prime targets for thieves. Often they are simply after the equipment itself and are not aware of the value of the data on the hard drive. The growing trend in identity theft and the ease of acquiring removable memory and hard drives through commercial resell services such as eBay® is quickly compounding the risks to these devices from casual thieves and dedicated criminals. Casual thieves simply resell it without regard for the data on the devices. Professional criminals and intelligence organizations are paying far more than the physical value of the drives in a gamble to obtain the sensitive data that is retrievable from these devices. It is a financial windfall for both at your expense.

A few common sense precautions can prevent the loss or theft of equipment and valuable data. Ensure that all mobile computing equipment is stored securely as possible when not in your personal possession. Use all available protection options for computer and network access. Keep all computers, and memory devices under close watch when in your personal possessions especially when traveling. Theft of computer equipment is often an opportunistic crime. Even a few moments of not paying attention can lead to lost machines, data, and careers.

While responsibility for valuable equipment and sensitive data is taken very seriously by the vast majority of Army personnel, there are far too many instances of Army computers and memory units found for sale in foreign markets. Some unscrupulous and opportunistic individuals seem to think that profit from the illegal sale of taxpayer-funded equipment is more important than the potential risk to American soldiers. These individuals will steal or otherwise misappropriate computer assets regardless of the value of the information, software or network portals they contain.

America was built on entrepreneurial spirit. Yet, all soldiers, civilian personnel and contractors should realize that the availability of U.S. Army equipment on the open market increases the chances of our enemies obtaining valuable intel on how to get past Army safeguards and gain access to sensitive information. There are too many threats to soldiers and their families already without giving the enemy extra opportunities for the sake of a few bucks. All Army personnel that are aware of government computer assets being waylaid for foreign marketplaces need to take whatever steps necessary to stop this practice. It's not a free market opportunity. It is putting Army lives, perhaps your own, at risk.